Ya XIAO, Zhi-jie FAN, Amiya NAYAK, Cheng-xiang TAN, 2019. Discovery method for distributed denial-of-service attack behavior in SDNs using a feature-pattern graph model. *Frontiers of Information Technology & Electronic Engineering*, 20(9):1195-1208.
https://doi.org/10.1631/FITEE.1800436

Discovery method for distributed denial-of-service attack behavior in SDNs using a feature-pattern graph model

Key words: Software-defined network; Distributed denial-of-service (DDoS); Behavior discovery; Distance metric learning; Feature-pattern graph

Corresponding author: Zhi-jie FAN
E-mail: aaronzfan@126.com
ORCID: https://orcid.org/0000-0002-7011-8632

Motivation

1. SDNs have many vulnerabilities generally because of the open framework. Among the well-known vulnerabilities of SDNs, DDoS attacks can have a devastating impact on the whole network, so more attention is required.
2. Because the traffic in SDNs is dynamic and attack approaches are complex nowadays, it is difficult to use the attack detection technology with only the traffic header information.
3. There are an increasing number of unknown attacks that SDNs cannot prevent; thus, it is challenging to automatically detect the unknown attacks.

Main idea

1. The proposed method models a feature-pattern graph (FPG) with link weight learning. The nodes represent various network patterns and the links between nodes denote the similarity. The graph model is scalable to updates and can be used in other attack scenarios.
2. A DDoS detection method is proposed based on the FPG.
3. A graph update model with both local and global updates is proposed to extend FPG and help with the detection of new attacks.

Method

1. First, a feature-pattern graph is built with attack signatures.

2. After the creation of DDoS attack signatures in the SDN, we propose our attack detection module, which is built on neighborhood classification in a feature-pattern graph model. The module is divided into two sub-modules, i.e., graph creation and detection engine.

Major results

1. The average prediction, recall, and *F*-score for two types of classification

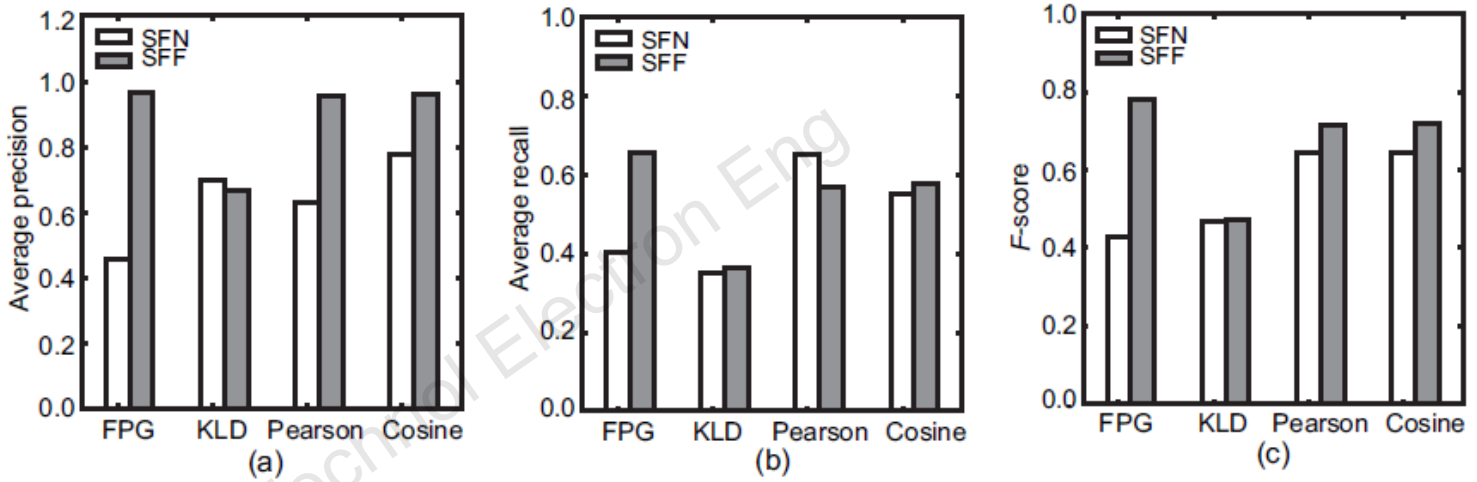

Fig. 5 Average precision (a), recall (b), and F-score (c) of multi-class prediction

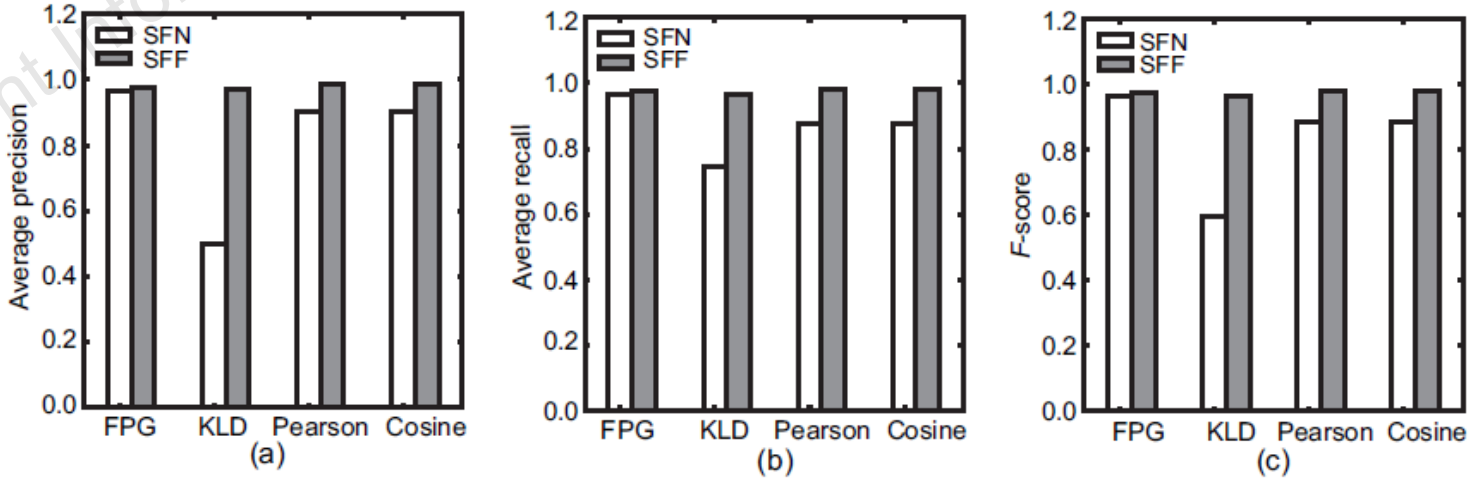

Fig. 6 Average precision (a), recall (b), and F-score (c) of binary class prediction

Major results (Cont'd)

2. Performance of the local and global updates

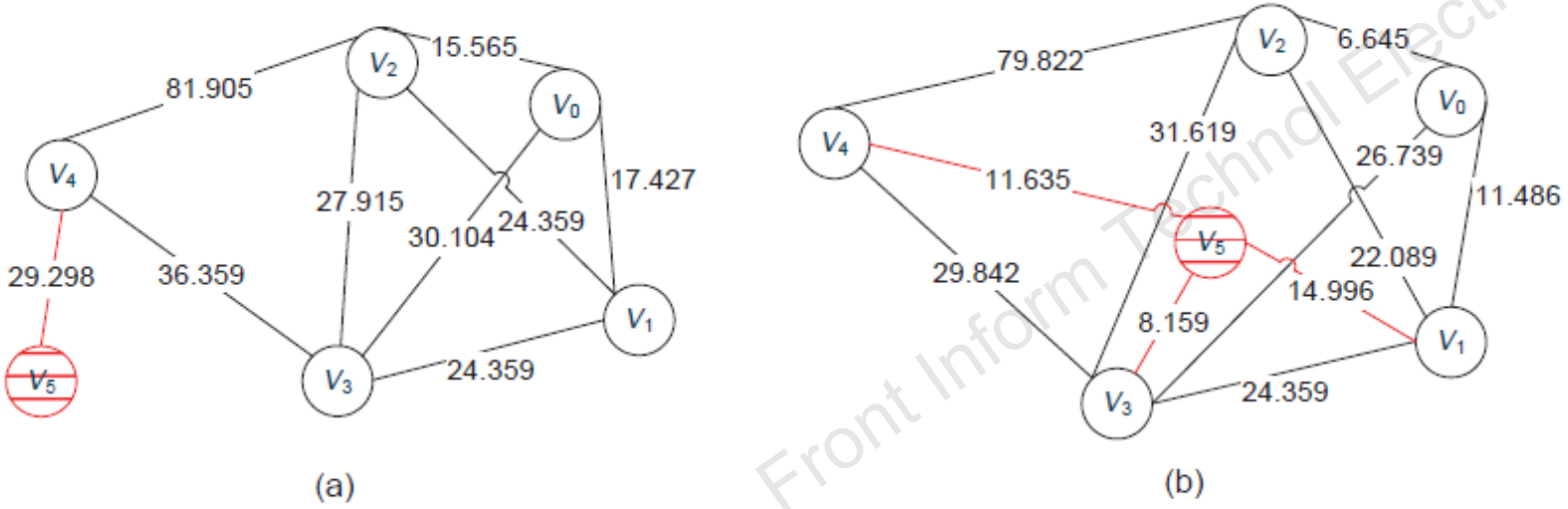

Fig. 7 Graph generated by local (a) and global (b) update

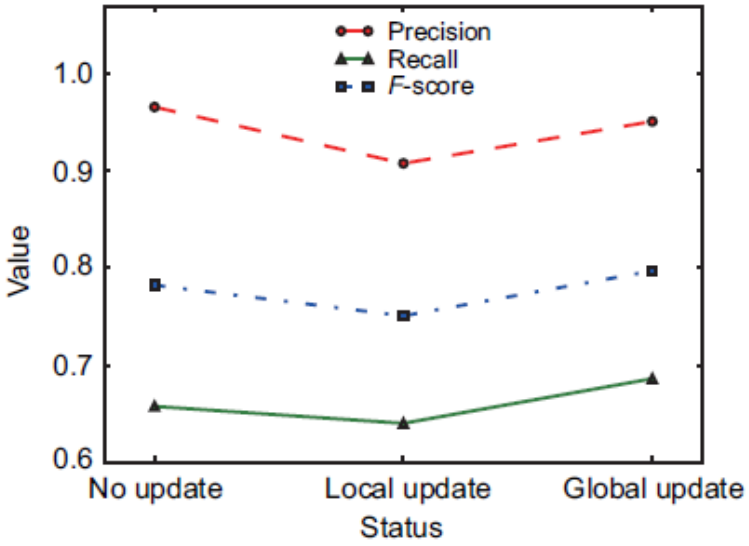

Fig. 8 Detection performance after graph update

Conclusions

1. A discovery method for distributed denial-of-service attack behaviors in SDNs using a feature-pattern graph model has been proposed.

2. Attack signatures have been created to adapt to the SDN environment through flow creation with the dataset from the traditional network and SDN traffic. A feature-pattern graph has been modeled based on the attack signatures.

3. The results of the experiments demonstrated that the feature-pattern graph based discovery method for DDoS attack behaviors substantially outperforms the compared methods on precision, recall, and *F*-score. Results from graph update verified the effectiveness of the local and global update approaches.